Department of Corrections **ADMINISTRATIVE BULLETIN** **Subject: INFORMATION SECURITY INCIDENTS**	**Number:** **03-01** **Date Issued:** **May 1, 2003** **Cancelled Effective:**

The purpose of this Administrative Bulletin (AB) is to announce a change of policy regarding the reporting of information security incidents. This policy change shall supersede current Department Operations Manual (DOM), Chapter 4, Article 44, Section 49010.6.5, Information Security Incident Report To DOF (refer to inset below).

49010.6.5 Information Security Incident Report To DOF

A report of major incidents as illustrated in SAM 4845 shall be submitted to OIT within ten working days of the Department's first awareness of an incident involving one or more of the following:

- Unauthorized intentional release, modification, or destruction of confidential or sensitive information, or the theft of such information including information stolen in conjunction with the theft of a computer or data storage device.
- Use of a State information asset in the commission of a crime.
- Intentional damage or destruction of State information assets, or the theft of such assets with an estimated value in excess of $500.

The report shall be signed by the Department Director and the Department Information Security Officer.

The current procedure calls for incidents to be reported through the chain of command to the Chief Deputy Directors and to the Department Information Security Officer (ISO).

These reporting requirements have recently been changed by the Department of Finance in Budget Letter 03-03. The changes expand the nature of incidents that shall be reported, and considerably shorten the reporting time frame from ten days to one day. Information security violations and incidents that are reportable have been newly defined as:

- Unauthorized access to, or modification of, State-owned or State-managed data, including nonelectronic data such as reports, documentation, and hard copy files.
- Unauthorized use of, or access to, State computer resources, including computer networks and services, as well as systems not necessarily connected to a network.

- Unauthorized access to, or modification of, computer software, including operating systems, networks, configurations and applications. This includes the introduction of malicious software such as viruses, worms, and other malicious software.
- Deliberate or unauthorized acts resulting in disruption of State computer services, including Denial of Service attacks.
- Unauthorized use of user account or Internet domain names.
- Destruction of, or damage to, State information processing facilities.
- Break-in or other unauthorized access to State facilities resulting in compromise to the data or computer systems housed within those facilities.

Should a situation occur, or staff become aware of a violation of State and departmental information security policies, an Information Security Incident Report shall be completed and submitted through the appropriate chain of command to the Chief Deputy Directors and to the ISO. The incident report shall be submitted within one business day of the discovery of the incident or situation.

A copy of the Information Security Incident Report is attached (see Attachment A). An electronic version of this report is available from the Information Security Unit link on the departmental web page, www.corr.ca.gov and from the Intranet site. Instructions for completion of the report are available at the same links.

In addition to information security incidents that fit any of the above criteria, new legislation requires additional measures be taken as well. Senate Bill 1386 and Assembly Bill 700, companion bills approved during the 2001/02 legislative session, impose new reporting requirements if the confidentiality of an individual's personal information is believed to have been breached. These new reporting requirements come into effect July 1, 2003, and they will apply to all systems maintained throughout the Department of Corrections that contain an individual's personal information. The full text of both bills may be found on the legislative web site at www.leginfo.ca.gov.

The laws state that these reporting requirements apply to any system containing individuals' first names or initials in conjunction with their last names, and any one of the following other data fields:

Department of Corrections **ADMINISTRATIVE BULLETIN** **Subject: INFORMATION SECURITY INCIDENTS**	**Number:**
	Date Issued:
	Cancelled Effective:

- Social Security Number.
- Driver License or California Identification Card Number.
- Account or credit card number(s) in conjunction with security, access, or password code required for access to financial records.

If a breach occurs or is believed to have occurred, all individuals whose personal information was compromised, or believed to have been compromised, shall be notified in writing, e-mail, or notice on the web page of that event. The notification shall include the date the breach occurred or was discovered.

To ensure the ability for a timely response in the event of an actual or suspected incident, it is advisable to review all systems and identify those to which these reporting requirements apply. Confidential, personal, and sensitive information, such as but not limited to, staff addresses, social security numbers, and home telephone numbers, should be protected. Each division/institution should maintain an inventory of those computers that are used to store confidential, personal, and sensitive information. Protective measures should be taken to ensure only authorized access to files, computers, and systems. These measures include logging off or activating screensaver/user ID access control when you leave your work area, not sharing or writing down your passwords, encrypting files containing confidential or sensitive information, and using email only for nonconfidential messages.

Please inform all concerned persons of this AB which shall remain in effect until incorporated into DOM, Chapter 4, Article 44. If you have any questions concerning the new reporting requirements or how to complete an Information Security Incident Report, contact Debborah Martin, Information Security Officer, Policy and Evaluation Division, at (916) 358-2459.

KATHY M. KINSER
Chief Deputy Director
Support Services

Attachment